CreateFile-02

Don't rely on HIDDEN, INDEXED, and ARCHIVE for file security

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-03-20

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 6434 bytes

Attack Category	Privilege Exploitation		
Vulnerability Category	Access Control		
Software Context	File Creation		
Location	• winbase.h		
Description	The CreateFile function creates or opens a file, file stream, directory, physical disk, volume, console buffer, tape drive, communications resource, mailslot, or named pipe. The function returns a handle that can be used to access an object.		
	Attributes HIDDEN, INDEXED, and ARCHIVE d not provide useful protection for secure files. Do not expect any useful security properties out of FILE_ATTRIBUTE_HIDDEN, FILE_ATTRIBUTE_NOT_CONTENT_INDEXED or FILE_ATTRIBUTE_ARCHIVE. Specifically, do not use FILE_ATTRIBUTE_HIDDEN to disguise your file. Use file and directory SECURITY_ATTRIBUTES.		
	Furthermore, FILE_ATTRIBUTE_NOT_CONTENT_INDEXED is simply a hint (not an enforceable mandate) to indexing software.		
	Finally, do not expect that setting FILE_ATTRIBUTE_ARCHIVE low will prevent back-up software from sending your secret data to tape. Its use has varied, but it is typically used by backup software to mark a file as backed up.		
APIs	FunctionName Comments		
	CreateFile		
Method of Attack	Setting File Attributes to HIDDEN, INDEXED, or ARCHIVE will not increase the security of your application. Do not expect them to.		
Exception Criteria			

^{1.} http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

CreateFile-02

Solutions	Solution Applicability	Solution Description	Solution Efficacy
		Follow guidance in Description. The creation disposition settings are often misinterpreted as to their inherent meaning with respect to security implications. "Hidden" does not necessarily imply "secure". Setting and manipulation of the security attributes is necessary to achieve security goals.	
Signature Details	HANDLE CreateFile(LPCTSTR lpFileName, DWORD dwDesiredAccess, DWORD dwShareMode, LPSECURITY_ATTRIBUTES lpSecurityAttributes, DWORD dwCreationDisposition, DWORD dwFlagsAndAttributes, HANDLE hTemplateFile);		
Examples of Incorrect Code	<pre>/* The setting of the FILE_ATTRIBUTES_HIDDEN, by design, does not secure files that you */ /* really to be secure; secure /= hidden */ [] HANDLE hFile = CreateFile(strMetaFile, GENERIC_WRITE, FILE_SHARE_READ, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL);</pre>		

```
if ( hFile ==
INVALID_HANDLE_VALUE )
{
CreateDirectory( strMetaFolder,
NULL );
SetFileAttributes( strMetaFolder,
FILE_ATTRIBUTE_HIDDEN );
hFile = CreateFile( strMetaFile,
GENERIC_WRITE,
FILE_SHARE_READ,
NULL,
CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL,
NULL );
```

Examples of Corrected Code

```
// Instead manipulation of the
security attributes is necessary
// such as
SECURITY_ATTRIBUTES sa;
// Set up security attributes to
allow
// inheritance of the file handle
sa.nLength =
sizeof(SECURITY_ATTRIBUTES);
sa.lpSecurityDescriptor = 0;
sa.bInheritHandle=TRUE;
STARTUPINFO startUpInfo;
PROCESS_INFORMATION procInfo;
BOOL success;
char s[100];
SECURITY_ATTRIBUTES sa;
// Set up security attributes to
not allow
// inheritance of the file handle
sa.nLength =
sizeof(SECURITY_ATTRIBUTES);
sa.lpSecurityDescriptor = 0;
sa.bInheritHandle=FALSE;
// Create a file handle
sample = CreateFile("parent.cpp",
GENERIC_READ,
FILE_SHARE_READ,
&sa,
OPEN_EXISTING,
FILE_ATTRIBUTE_NORMAL,
if (sample==INVALID_HANDLE_VALUE)
cout << "In CreateFile" <<</pre>
GetLastError()
<< endl;
```

CreateFile-02 ID: 718-BSI | Version: 3 | Date: 5/16/08 2:39:17 PM

Source Reference	_	• http://msdn.microsoft.com/library/default.asp? url=/library/en-us/fileio/base/createfile.asp ²		
Recommended Resource				
Discriminant Set	Operating System	• Windows		
	Languages	• C		
		• C++		

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about "Fair Use," contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

CreateFile-02

ID: 718 PST | Various 3 | Data 5/16/08 3:30:17 PM

^{1.} mailto:copyright@cigital.com